

Plotkin construction: Rank and Kernel*

J. Borges, C. Fernández

Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autònoma de Barcelona
08193 Bellaterra, Spain

February 1, 2008

Abstract

Given two binary codes of length n , using Plotkin construction we obtain a code of length $2n$. The construction works for linear and nonlinear codes. For the linear case, it is straightforward to see that the dimension of the final code is the sum of the dimensions of the starting codes. For nonlinear codes, the rank and the dimension of the kernel are standard measures of linearity. In this report, we prove that both parameters are also the sum of the corresponding ones of the starting codes.

Keywords: Plotkin construction, rank, kernel, codes.

Introduction

Let \mathbb{F}^n be the vector space of dimension n over \mathbb{Z}_2 . The Hamming distance between vectors $x, y \in \mathbb{F}^n$, denoted by $d(x, y)$, is the number of coordinates in which x and y differ. A binary code C of length n is a subset of \mathbb{F}^n , its elements are called codewords. The minimum distance of a code C is the minimum of the distances between pairs of different codewords.

Let C be a binary code. If C is a subspace of \mathbb{F}^n , then we say that C is a $[n, k, d]$ linear code, where k is the dimension of C and d is its minimum distance. If C is not a subspace, we say that is a nonlinear $(n, |C|, d)$ code.

Given a binary code C , the *rank* of C is defined as the dimension of the linear span of C . I.e. $rank(C) = \dim\langle C \rangle$. The *kernel* of a binary code C , $Ker(C)$, is the set of vectors that leave C invariant under translation, i.e. $Ker(C) = \{x \in \mathbb{F}^n \mid C + x = C\}$. If C contains the all-zero vector, then $Ker(C)$ is a linear subcode of C . Note that for a linear code, the rank and the dimension of the kernel are simply the dimension of the code.

*This work has been partially supported by the Spanish MEC and the European FEDER MTM2006-03250 Grant and by the PNL2006-13UAB Grant.

Let C_1 and C_2 be two binary codes of length n . We can construct a binary code C of length $2n$ by terms of C_1 and C_2 with the following construction:

$$C = \{(u|u+v) : u \in C_1, v \in C_2\}, \quad (1)$$

where $|$ denotes concatenation. Such construction is called Plotkin construction or $(u|u+v)$ -construction and was first stated by Plotkin in 1960 [1].

Let C_1 and C_2 be binary codes and let C be the code obtained using construction (1).

- If C_1 and C_2 are linear $[n, k_1, d_1]$ and $[n, k_2, d_2]$ codes then, C is a linear $[2n, k_1 + k_2, \min\{2d_1, d_2\}]$ code.
- If C_1 and C_2 are nonlinear $(n, |C_1|, d_1)$ and $(n, |C_2|, d_2)$ codes then, C is a nonlinear $(2n, |C_1| \cdot |C_2|, \min\{2d_1, d_2\})$ code.

Theorem 1 *Let C_1 and C_2 be binary codes of length n , $\mathbf{0} \in C_1$, $\mathbf{0} \in C_2$, and let C be the binary code built from them via construction (1). Therefore,*

$$(i) \text{ Ker}(C) = \{(x|x+y) : x \in \text{Ker}(C_1), y \in \text{Ker}(C_2)\},$$

$$(ii) \langle C \rangle = \{(x|x+y) : x \in \langle C_1 \rangle, y \in \langle C_2 \rangle\}.$$

Proof:

- (i) For any $x \in \text{Ker}(C_1), y \in \text{Ker}(C_2), (u|u+v) \in C$ we obtain $(x|x+y) + (u|u+v) = (x+u|(x+u)+(y+v)) \in C$. Thus, $(x|x+y) \in \text{Ker}(C)$.

Now, let $(x|x+y) \in \text{Ker}(C)$. For any $u \in C_1$ and $v \in C_2$, we have $(u|u+v) \in C$ and $(x|x+y) + (u|u+v) = (x+u|(x+u)+(y+v)) \in C$. By construction, $x+u \in C_1$ and, therefore, $x \in \text{Ker}(C_1)$. To prove that $y \in \text{Ker}(C_2)$ we consider $v \in C_2$ and the codeword $(x|x+v) \in C$. Then, since $(x|x+y) + (x|x+v) = (\mathbf{0}|\mathbf{0} + (y+v)) \in C$ we conclude that $y+v \in C_2$ and $y \in \text{Ker}(C_2)$.

- (ii) Let $x = \sum_{i=1}^s u_i \in \langle C_1 \rangle, y = \sum_{j=1}^t v_j \in \langle C_2 \rangle$, where $u_i \in C_1$, for $i = 1, \dots, s$, $v_j \in C_2$, for $j = 1, \dots, t$. Then $(x|x+y) = \sum_{i=1}^s (u_i|u_i + \mathbf{0}) + \sum_{j=1}^t (\mathbf{0}|\mathbf{0} + v_j) \in \langle C \rangle$.

Finally, if $(x|x+y) \in \langle C \rangle$ then $(x|x+y) = \sum_{i=1}^k (u_i|u_i + v_i) = (\sum_{i=1}^k u_i | (\sum_{i=1}^k u_i) + (\sum_{i=1}^k v_i))$, where $x = \sum_{i=1}^k u_i \in \langle C_1 \rangle$ and $\sum_{i=1}^k v_i \in \langle C_2 \rangle$.

■

Corollary 2 *With the same conditions as in Theorem 1*

$$(i) \dim(\text{Ker}(C)) = \dim(\text{Ker}(C_1)) + \dim(\text{Ker}(C_2)),$$

$$(ii) \text{rank}(C) = \text{rank}(C_1) + \text{rank}(C_2).$$

Proof: It is easy to check that $f : \text{Ker}(C_1) \times \text{Ker}(C_2) \rightarrow \text{Ker}(C), f(x, y) = (x|x+y)$ and $g : \langle C_1 \rangle \times \langle C_2 \rangle \rightarrow \langle C \rangle, g(x, y) = (x|x+y)$ are bijections. Therefore:

$$(i) |\text{Ker}(C)| = |\text{Ker}(C_1)| \cdot |\text{Ker}(C_2)| \text{ and } \dim(\text{Ker}(C)) = \dim(\text{Ker}(C_1)) + \dim(\text{Ker}(C_2)).$$

$$(ii) |\langle C \rangle| = |\langle C_1 \rangle| \cdot |\langle C_2 \rangle| \text{ and } \text{rank}(C) = \text{rank}(C_1) + \text{rank}(C_2).$$

■

References

- [1] M. Plotkin. “Binary codes with specified minimum distances,” *IEEE Trans. Inform. Theory*, vol. 6, pp. 445-450, 1960.